Einspruch gegen ein europäisches Patent

An das
Europäische Patentamt

Tabulatoren-Positionen

nur für EPA

I. Angegriffenes Patent EPO - Munich 88

13. März 2008

Einspr.-Nr. OPPO (1)

Patentnummer	1 384 369
Anmeldenummer	02745226.7
Tag des Hinweises auf Erteilung (Art. 97(4), 99(1) EPÜ)	13.06.2007

Bezeichnung der Erfindung (Titel):

Verfahren und System für den Aufbau einer Verbindung zwischen einem Personal Security Device und einem Fernrechnersystem

II. In der Patentschrift als erster/einziger genannter

Patentinhaber Activcard Ireland Limited
Dublin 2 (IE)

Zeichen des Einsprechenden oder Vertreters (maximal 15 Positionen) 50 0809/bof-hot OREF

III. Einsprechender OPPO (2)

Name Giesecke & Devrient GmbH

Anschrift Prinzregentenstraße 159
81677 München

Staat des Wohnsitzes oder Sitzes Deutschland

Telefon/Telex/Telefax 089/4119-1680 — 089/4119-1399

Gemeinsamer Einspruch ☐ Miteinsprechende siehe Zusatzblatt

IV. Bevollmächtigung OPPO (9)

1. **Vertreter**
(Nur einen Vertreter angeben, dem zugestellt werden soll)

Name

Geschäftsanschrift

Telefon/Telex/Telefax

Weitere zugelassene Vertreter ☐ (siehe Zusatzblatt/Vollmacht) OPPO (5)

2. **Angestellte(r)** des Einsprechenden, die/der für dieses Einspruchsverfahren gemäß Art. 133(3) EPÜ bevollmächtigt werden/wird

Name(n): Frank Bornhäuser

Vollmacht(en)

Zu 1./2.

☐ nicht erforderlich
☒ registriert unter Nr. 505380.8
☐ beigefügt

nur für EPA

V. Der Einspruch richtet sich gegen das erteilte Patent

— im gesamten Umfang [X]

— im Umfang der Ansprüche Nr.

VI. Einspruchsgründe:

Der Einspruch wird darauf gestützt, daß

(a) der Gegenstand des europäischen Patents nicht patentfähig ist (Art. 100(a) EPÜ), weil er

— nicht neu ist (Art. 52(1); 54 EPÜ) [X]

— nicht auf einer erfinderischen Tätigkeit beruht (Art. 52(1); 56 EPÜ) [X]

— aus sonstigen Gründen nämlich Art. [ ] [ ]

von der Patentierbarkeit ausgeschlossen ist.

(b) das europäische Patent die Erfindung nicht so deutlich offenbart, daß ein Fachmann sie ausführen kann (Art. 100(b) EPÜ, vgl. Art. 83 EPÜ). [ ]

(c) der Gegenstand des europäischen Patents über den Inhalt der Anmeldung/der früheren Anmeldung in der ursprünglich eingereichten Fassung hinausgeht (Art. 100(c) EPÜ, vgl. Art. 123(2) EPÜ). [ ]

VII. Tatsachenvorbringen und Begründung

(Regel 55(c) EPÜ)
erfolgt auf gesondertem Schriftstück (Anlage 1) [X]

VIII. Sonstige Anträge:

Mündliche Verhandlung wird beantragt, falls das angegriffene Patent nicht allein aufgrund der schriftlichen Ausführungen im beantragten Umfang widerrufen werden kann.

IX. Beweismittel

Beigeschlossen = X

wird / werden nachgereicht =

nur für EPA

A. **Veröffentlichungen:**

Datum der Veröffentlichung

1 D3: WO 98/52150 A1

Besonders relevant (Seite/Spalte/Zeile/Fig.):

2 D4: WO 96/34483 A1

Besonders relevant (Seite/Spalte/Zeile/Fig.):

3 D5: DE 199 47 986 A1

Besonders relevant (Seite/Spalte/Zeile/Fig.):

4 D6: EP 0 895 204 A2

Besonders relevant (Seite/Spalte/Zeile/Fig.):

5 D7: CA 2 330 534

Besonders relevant (Seite/Spalte/Zeile/Fig.):

6 D8: US 6 196 459 B1

Besonders relevant (Seite/Spalte/Zeile/Fig.):

7 D9: Global Platform, Multi Application - Smart Card Management Systems, Version 3.3 November 2000

Besonders relevant (Seite/Spalte/Zeile/Fig.):

Fortsetzung auf Zusatzblatt X

B. **Sonstige Beweismittel**

Weitere Angaben auf Zusatzblatt ☐

X. Zahlung der Einspruchsgebühr erfolgt

nur für EPA

☒ wie auf beigefügtem Gebührenzahlungsvordruck (EPA Form 1010) angegeben

☐

XI. Liste der Unterlagen:

Anlage Nr.:		Stückzahl:		
0	☒ Einspruchsformblatt	2	(mind. 2)	
1	☒ Tatsachen und Begründung (s. VII.)	2	(mind. 2)	
2	Kopien von als Beweismittel angegebenen (s. IX.)			
2a	☒ — Veröffentlichungen	2	(mind. je 2)	
2b	☐ — sonstigen Unterlagen		(mind. je 2)	
3	☐ Unterzeichnete Vollmacht(en) (s. IV.)			
4	☒ Gebührenzahlungsvordruck (s. X.)	1		
5	☐ Scheck			
6	☒ Zusatzblatt (Zusatzblätter)	2	(mind. je 2)	
7	☐ Sonstige Unterlagen (bitte einzeln anführen):			

XII. Unterschrift des Einsprechenden oder Vertreters

Ort München

Datum 13.03.08

F. Bomhäuser
Nr. 505360.8

Gleiche & Devrient GmbH

Name des (der) Unterzeichneten bitte mit Schreibmaschine wiederholen. Bei juristischen Personen bitte die Stellung des (der) Unterzeichneten innerhalb der Gesellschaft mit Schreibmaschine angeben

Begründung

I. Angeführte Dokumente

Der Einspruch stützt sich auf die folgenden Entgegenhaltungen:

D3: WO 98/52150 A1,

D4: WO 96/34483 A1,

D5: DE 199 47 986 A1,

D6: EP 0 895 204 A2,

D7: CA 2 330 534,

D8: US 6 196 459 B1,

D9: Global Platform, Multi Application – Smart Card Management Systems, Version 3.3 November 2000,

D10: Handbuch der Chipkarten, Rankl/Effing, 3. Auflage - 1999, insbesondere S. 622-640 und

D11: ETSI TS 101 181, v 8.3.0 (2000-08), Security Mechanisms for the SIM application toolkit.

Weiterhin wird Bezug genommen auf das bereits im Prüfungsverfahren genannte Dokument:

D1: WO 99/62210 A2.

II. Gegenstand des Streitpatents (EP 1 384 369 B1)

Der Gegenstand der unabhängigen Patentansprüche 1 und 10 des Streitpatents wird im Folgenden nach Merkmalen gegliedert dargestellt.

Gemäß Absatz [0008] des Streitpatents soll durch den beanspruchten Gegenstand ein Verfahren angegeben werden, welches das Aufbauen einer Verbindung von einem entfernten Computersystem zu einer Sicherheitseinrichtung (PSD) erlaubt, ohne dass auf dem Client eine Software zur Übersetzung der Datenpakete von einem Format einer höheren Schicht (High-Level-Format) in ein Format einer niedrigeren Schicht (PSD-Format) benötigt wird.

Der unabhängige Anspruch 1 enthält eine Vielzahl von Verfahrensschritten, die sich auf das Computersystem (a-d; k-m), den Client (e-f; i-j) und das PSD (g,h) beziehen und sich dabei sowohl auf den Hinweg der Datenpakete (a-f) als auch auf den Rückweg der Antworten hierauf (g-m) beziehen. Der unabhängige Anspruch 10 ist dagegen nur auf das Computersystem gerichtet.

Die angeblich neue Idee, die in diesen beiden Ansprüchen enthalten ist, ist das Konvertieren der Datenpakete in das PSD-Format auf dem Computersystem. Im Client können die Datenpakete dadurch transparent zum PSD weiter gereicht werden (siehe Absatz [0010] des Streitpatents).

1. Verfahren zum Aufbauen einer Kommunikations-Pipeline zwischen mindestens einer PSD (40) und mindestens einem Remotecomputersystem (50) über ein Netz (45), das mindestens einen Client (10) als Host für die mindestens eine PSD (40) verwendet, wobei der mindestens eine Client (10) und das mindestens eine Remotecomputersystem (50) unter Verwendung eines Paket-basierten Kommunikationsprotokolls über das Netz (45) in funktionaler Kommunikation stehen, wobei das Verfahren umfasst:

a - Erzeugen oder Abrufen in dem mindestens einen Remotecomputersystem (50) einer Anfrage (200; 500), um auf die mindestens eine PSD (40) zuzugreifen, wobei die Anfrage (200; 500) in einem High-Level-Nachrichtenformat vorliegt,

b - Konvertieren der Anfrage (200; 500) in dem mindestens einen Remotecomputersystem (50) von dem High-Level-Nachrichtenformat in eine Anfragenachricht, die PSD-formatiert ist, um eine PSD-formatierte Anfragenachricht (220; 520) zu erzeugen,

c - Einkapseln der PSD-formatierten Anfragenachricht (220; 520) in dem mindestens einen Remotecomputersystem (50) mit dem Paket-basierten Kommunikationsprotokoll, wodurch eine eingekapselte PSD-formatierte Anfragenachricht (210; 530) erstellt wird,

d - Übermitteln (230, 240; 535, 540) der eingekapselten PSD-formatierten Anfragenachricht (210; 530) unter Verwendung des Paket-basierten Kommunikationsprotokolls von dem mindestens einen Remotecomputersystem (50) an den mindestens einen Client (10) über das Netz (45),

e - Extrahieren der PSD-formatierten Anfragenachricht (260, 270; 560, 570) von der eingekapselten PSD-formatierten Anfragenachricht (250; 550) in dem mindestens einen Client (10),

f - Übermitteln der PSD-formatierten Anfragenachricht (260, 270; 560, 570) von dem mindestens einen Client (10) an die mindestens eine PSD (40),

g - Verarbeiten der PSD-formatierten Anfragenachricht (260, 270; 560, 570) wodurch eine PSD-formatierte Antwortnachricht (360, 370; 660, 670) erstellt wird,

h - Übermitteln der PSD-formatierten Antwortnachricht (360, 370; 660, 670) von der mindestens einen PSD (40) an den mindestens einen Client (10),

i - Einkapseln in dem mindestens einen Client (10) der PSD-formatierten Antwortnachricht (360, 370; 660, 670) mit dem Paket-basierten Kommunikationsprotokoll, sodass eine eingekapselte PSD-formatierte Antwortnachricht (350; 650) erstellt wird,

j - Übermitteln (330, 340; 635; 640) der eingekapselten PSD-formatierten Antwortnachricht (350; 650) unter Verwendung des Paket-basierten Kommunikationsprotokolls von dem mindestens einen Client (10) an das mindestens eine Remotecomputersystem (50) über das Netz (45),

k - Extrahieren der PSD-formatierten Antwortnachricht (320; 630) von der eingekapselten PSD-formatierten Antwortnachricht (310; 610) in dem mindestens einen Remotecomputersystem (50),

l - Konvertieren der PSD-formatierten Antwortnachricht (320; 630) in eine High-Level-Antwortnachricht (300; 600) in dem mindestens einen Remotecomputersystem (10) und

m - Verarbeiten der High-Level-Antwortnachricht in dem mindestens einen Remotecomputersystem (50).

10. Remotecomputersystem (50) zum Einrichten einer Kommunikationspipeline zwischen mindestens einer PSD (40) und dem Remotecomputersystem (50) über ein Netz (45) unter Verwendung eines Clients (10) als Host für die mindestens eine PSD (40), wobei das Remotecomputersystem umfasst:

A - Remotecomputersystem-Kommunikationsmittel (105S) zum Übermitteln und Empfangen von Nachrichten über das Netz unter Verwendung eines Paket-basierten Kommunikationsprotokolls,

B - Erste Remotecomputersystem-Datenverarbeitungsmittel (55) zum Konvertieren PSD-formatierter Nachrichten in High-Level-Nachrichten und umgekehrt,

C - Zweite Remotecomputersystem-Datenverarbeitungsmittel (100) zum Implementieren von High-Level-Programmen,

D - Dritte Remotecomputersystem-Datenverarbeitungsmittel (70) umfassend:

d1 - Mittel zum Empfangen eingehender Nachrichtenpakete (310; 610) über das Netz (45) unter Verwendung der Remotecomputersystem-Kommunikationsmittel (105S) zum Extrahieren eingehender PSD-formatierter Nachrichten (320; 630) von den eingehenden Nachrichtenpaketen (310; 610) und zum Übermitteln der eingehenden PSD-formatierten Nachrichten (320; 630) an die zweiten Remotecomputersystem-Datenverarbeitungsmittel (100) durch die ersten Remotecomputersystem-Datenverarbeitungsmittel (55) und

d2 - Mittel zum Empfangen ausgehender PSD-formatierten Nachrichten (220; 520), die von den zweiten Remotecomputersystem-Datenverarbeitungsmitteln (100) durch die dritten Remotecomputersystem-Datenverarbeitungsmittel (55) kommen, zum Einkapseln der ausgehenden PSD-formatierten Nachrichten (220; 520) in ausgehende Nachrichtenpakete (210; 530) und zum Übermitteln der ausgehenden Nachrichtenpakete (210; 530) über das Netz (45) unter Verwendung der Remotecomputersystem-Kommunikationsmittel (105S).

III. Fehlende Neuheit der unabhängigen Patentansprüche gegenüber WO 98/52150 A1 (D3)

Die unabhängigen Patentansprüche des Streitpatentes sind nicht neu gegenüber der Offenbarung von WO 98/52150 A1 (D3).

Dokument D3 betrifft ein System zum Laden von Daten von einem Chipkarten-Administrations-System CAS auf eine Chipkarte CC über ein Chipkarten-Kontroll-System CKS. Chipkartenkommandos und -antworten werden dabei, wie in Figur 2 erkennbar, transparent zwischen dem Administrationssystem CAS und der Karte CC übertragen. Der Ansatz einer transparenten Übertragung von Kommandos, die in einem entfernten System erzeugt werden ist also bekannt (siehe auch Zusammenfassung von D3).

Zu Anspruch 1:
Im einzelnen zeigt das Dokument ein Verfahren zum Aufbauen einer Kommunikations-Pipeline (siehe Seite 3, vorletzter Absatz) zwischen mindestens einer Chipkarte CC als PSD und mindestens einem Administrationssystem CAS als Remote-Computersystem über ein Netz, das mindestens ein Chipkartenkontrollsystem CKS (Client) als Host für die mindestens eine PSD verwendet, wobei der mindestens eine Client CKS und das mindestens eine Remotecomputersystem CAS unter Verwendung eines Paket-basierten Kommunikationsprotokolls über das Netz (LAN oder WAN, siehe Seite 14, Zeile 7 ff) in funktionaler Kommunikation stehen (siehe Zusammenfassung und Figur 2).

Im Sinne von Merkmal a erhält das mindestens eine Remotecomputersystem CAS eine Personalisierungsanfrage (siehe Figur 2), um auf die mindestens eine PSD CC zuzugreifen, wobei die Anfrage naturgemäß in einem „High-Level-Nachrichtenformat" vorliegt (d.h. sie ist nicht PSD-formatiert).

Im Sinne von Merkmal b wird die Anfrage in dem Remotecomputersystem CAS von dem High-Level-Nachrichtenformat in eine Anfragenachricht „Chip Kommando"

(siehe Figur 2) konvertiert, die PSD-formatiert ist, um eine PSD-formatierte Anfragenachricht zu erzeugen (siehe beispielsweise letztes Merkmal von Anspruch 1 und Seite 15, vierter Absatz „ ... das CAS erzeugt die Personalisierungskommandos ... ").

Dass das Datenpaket „Chip Kommando" im Sinne von Merkmal c zur Übertragung über das LAN/WAN in dem Remotecomputersystem CAS in das entsprechende Paket-basierten Kommunikationsprotokoll eingekapselt werden muss, wodurch eine eingekapselte PSD-formatierte Anfragenachricht erstellt wird, ist bereits durch die Existenz des Netzes vorgegeben aber hier auch explizit beschrieben (siehe Seite 6, dritter und vierter Absatz).

Wie in Merkmal d dargestellt, wird also die eingekapselte PSD-formatierte Anfragenachricht unter Verwendung des Paket-basierten Kommunikationsprotokolls von dem mindestens einen Remotecomputersystem CAS an den mindestens einen Client CKS über das Netz übermittelt (siehe Figur 2 und ggf. Seite 9 zweiter Absatz).

Um das Chipkommando transparent weiterleiten zu können, muss auch in Dokument D3 im Client CKS im Sinne von Merkmal e die PSD-formatierte Anfragenachricht „Chip Kommando" von der eingekapselten PSD-formatierten Anfragenachricht extrahiert werden.

Der Client CKS übermittelt die PSD-formatierten Anfragenachricht an das PSD CC im Sinne von Merkmal f (siehe auch letztes Merkmal von Anspruch 7 in Dokument D3).

Da die Karte CC als PSD, wie es jede Karte tut, im Sinne von Merkmal h eine PSD-formatierte Antwort „Chip Antwort" (siehe Figur 2) in Reaktion auf das Kommando sendet, hat sie das Kommando als PSD-formatierten Anfragenachricht im Sinne von Merkmal g auch verarbeitet und die entsprechende Antwortnachricht erstellt.

Analog zu den Merkmalen c bis e muss die PSD-formatierte Antwortnachricht „Chip

Antwort" für die Übertragung über das Netz im Sinne von Merkmal i in dem Client CKS mit dem Paket-basierten Kommunikationsprotokoll eingekapselt werden, sodass eine eingekapselte PSD-formatierte Antwortnachricht erstellt wird, im Sinne von Merkmal j die eingekapselte PSD-formatierte Antwortnachricht unter Verwendung des Paket-basierten Kommunikationsprotokolls von dem mindestens einen Client CKS an das mindestens eine Remotecomputersystem CAS über das Netz übertragen werden und im Sinne von Merkmal k die PSD-formatierte Antwortnachricht „Chip Antwort" von der eingekapselten PSD-formatierten Antwortnachricht in dem mindestens einen Remotecomputersystem ausgepackt werden (siehe auch Seite 6 vierter Absatz „die vom CKS empfangenen Daten werden (im CAS) entpackt").

In dem Remotecomputersystem CAS läuft eine Steuerungssoftware mit einer „Ablauflogik" (siehe Seite 3, vierter Absatz), die vorgibt welche Kommandos in welcher Reichenfolge an die Karte CC zu senden sind und welche Antworten der Karte CC zu erwarten sind (siehe Seite 10 zweiter Absatz). Die Software des Remotecomputersystems CAS arbeitet nicht im PSD-Format (sondern in einem High-Level-Format), die PSD-formatierte Antwortnachricht muss also in dem CAS in eine High-Level-Antwortnachricht konvertiert werden (Merkmal l). Beispielsweise wird aus der Standardantwort der Karte „90 00" in der Ablauflogik des CAS der Unterfall „Kommando erfolgreich", woraufhin als eine Form der Verarbeitung der High-Level-Antwortnachricht im Remotecomputersystem CAS im Sinne von Merkmal m das nächste Kommando gesendet werden kann (siehe Figur 2). Als weitere Ergebnisse einer zweifelsohne somit im CAS erfolgenden Verarbeitung der Antworten zeigt das Dokument im Falle eines Fehlers die Anforderung eines Resets (siehe Seite 10, zweiter Absatz und „Chip reset Anforderung" in Figur 2) und das Senden einer Abschlussnachricht nach erfolgreicher Übertragung aller Datenpakete (siehe Seite Teilschritt 6 auf Seite 11 und „Personalisierungs-Ergebnis" in Figur 2).

Soweit einzelne Details eines Merkmals in Dokument D3 nicht ausformuliert sein sollten, liest der Fachmann sie als Teil der dort beschriebenen Lösung jedoch mit. Insgesamt ist somit der Gegenstand von Anspruch 1 für den Fachmann aus Dokument D3 bekannt.

Zu Anspruch 10:
Anspruch 10 ist auf ein Remotecomputersystem gerichtet, welches die nötigen Mittel zur Durchführung der entsprechenden Verfahrensschritte (a-d; k-m) aus Anspruch 1 umfasst. Daher ist es nicht überraschend, dass auch dessen Lehre aus Dokument D3 bekannt ist.

Das Dokument zeigt mit dem Chipkarten-Administrationssystem CAS ein Remotecomputersystem zum Einrichten einer Kommunikationspipeline (siehe Seite 3 vorletzter Absatz) zwischen mindestens einer Chipkarte als PSD und dem Remotecomputersystem über ein Netz unter Verwendung eines Chipkarten-Kontroll-Systems CKS als Client, als Host für die mindestens eine PSD (siehe Figur 2).

Das CAS kann Nachrichten über das Netz unter Verwendung eines paket-basierten Kommunikationsprotokolls Übermitteln und Empfangen (siehe Figur 2 oder 3) und weist also ein Remotecomputersystem-Kommunikationsmittel (siehe auch Bezugszeichen 390 in Figur 3) im Sinne von Merkmal A auf.

Jeder moderne Computer, also auch das CAS, hat eine CPU und ein entsprechendes Betriebssystem und weist somit zweite Remotecomputersystem-Datenverarbeitungsmittel zum Implementieren von High-Level-Programmen im Sinne von Merkmal C auf.

Zum Austausch von Daten zwischen der Schnittstelle und den Programmen des CAS gibt es notwendigerweise dritte Remotecomputersystem-Datenverarbeitungsmittel im Sinne von Merkmal D, damit das Programm nicht alle Netzwerk-Schnittstellenformate selbst bereitstellen muss. Die Aufgabe der dritten Mittel ist im Sinne von Merkmal d1 aus bei dem Remotecomputersystem-Kommunikationsmittel über das Netz eingehenden Nachrichtenpaketen Nachrichten zu extrahieren und an die zweiten Remote-computersystem-Datenverarbeitungsmittel zu übermitteln. Analog werden gemäß Merkmal d2 ausgehende Nachrichten von dem Programm als zweiten Remotecomputersystem-Datenverarbeitungsmittel empfangen und in

ausgehende Nachrichtenpakete eingepackt, bevor Sie über das Netz unter Verwendung der Schnittstelle übermittelt werden können.

Nach diesseitigem Verständnis beschreiben die Merkmale A, C und D - hier ausgenommen PSD-formatierter Nachrichten - einen normalen netzwerkfähigen PC oder Server-Rechner.

Wenn nun, wie in Dokument D3, PSD-formatierte Nachrichten transparent über das Netz übertragen werden sollen, behandelt das dritte Datenverarbeitungsmittel auch PSD-formatierte Nachrichten als Nachrichten im Sinne des fehlenden Teilmerkmals aus Merkmal D.

Wie zuvor bereits für die Merkmale b und l aus Anspruch 1 festgestellt, weist das Chipkarten-Administrationssystem CAS als Remotecomputersystem auch Mittel auf, um im Sinne von Merkmal B PSD-formatierte Nachrichten in High-Level-Nachrichten und umgekehrt zu konvertieren.

Auch der Gegenstand von Anspruch 10 kann somit als durch die Lehre von Dokument D3 für den Fachmann vorweggenommen gelten.

Sollte man sich jedoch auf den Standpunkt stellen, dass nicht alle Merkmale von Anspruch 1 oder 10 aus Dokument D3 bekannt sind oder vom Fachmann zumindest dort mitgelesen werden, so würde der Fachmann für Software zur Kommunikation mit PSDs wie Chipkarten gegebenenfalls fehlende Elemente aus seinem Fachwissen ergänzen.

IV. Abhängige Patentansprüche

In keinem der abhängigen Ansprüche 2 – 9 oder 11 bis 15 des Streitpatents sind zusätzliche Merkmale enthalten, die neu sind und eine Erfindungshöhe begründen könnten.

Die zunächst angenommene Idee des Streitpatentes, bereits in einem entfernten Computersystem die Datenpakete in ein PSD-Format zu bringen, ist auch aus einer Vielzahl von weiteren Dokumenten bekannt. Bevor die wichtigsten Bezüge der weiteren relevanten Dokumente für die abhängigen Ansprüche aufgeführt werden, sollen im Folgenden die Dokumente jeweils kurz eingeführt werden.

IV.1 Weitere relevante Dokumente

WO 96 34483 A1 (D4)

Dokument D4 zeigt ein System 40 bestehend aus einem Serviceprovider 42 als entferntes Computersystem, welches über ein Netz 41 eine Verbindung zu einer Karte 11 in einem Client 1, 13 aufbaut (siehe Figur 7). Gemäß Anspruch 1 ist der Client angepasst, empfangene Daten transparent an die Karte weiter zu leiten.

Wie in Bezug auf Figur 6 auf Seite 15 in den Zeilen 12ff näher beschrieben, können Low-Level-Kommandos L mit einem Header versehen werden, um als High-Level-Kommandos H* übertragen werden zu können (Zeile 22-25, Seite 15). Das transparente Weiterleiten vermeidet dabei ein Update der Software im Client (siehe Seite 15, Z. 25 bis Zeile 3 auf Seite 16).

Angemerkt werden soll an dieser Stelle, dass zum Prioritätszeitpunkt quasi jedes Netz paket-basierte Kommunikationsprotokolle bereits stellt, da die ehedem nicht paket-basierten, sondern leitungsvermittelten Telekommunikationsnetze zum Prioritätszeitpunkt bereits ebenfalls paket-basierte Dienste anbieten (GPRS, UMTS, ...) und Computernetze wie Internet, LAN oder WAN per se paketbasiert arbeiten.

DE 199 47 986 A1 (D5)

In Dokument D5 wird, wie in Figur 3 und Figur 5 erkennbar, auf einem Server eine Kommandosequenz für eine Chipkarte erzeugt und über das Internet zu einem Client als Host der Chipkarte übertragen. Der Client packt die Kommandosequenz aus und sendet die signierten und verschlüsselten einzelnen Kommandos (transparent) an die Chipkarte.

EP 0 895 204 A2 (D6)

Das Dokument zeigt ein Personalisierungssystem für Chipkarten, in welchem eine Steuereinrichtung 11 Kommandos erzeugt und an eine Kartenausgabestation 21 überträgt, welche die Kommandos transparent an die Chipkarten weiterleitet (siehe Figur 1). Die auf dem Übertragungsweg gekapselten Kommandos und Antworten sind in Fig. 7, 8 und 9 dargestellt.

CA 2 330 534 (D7)

Dokument D7 ist eine ältere Anmeldung zumindest eines auch für das Streitpatents benannten Erfinders. In dieser Anmeldung werden die PSD-formatierte Kommandodaten für das PSD 31 erst in einem Client 1 erzeugt (siehe Figur 1). Das Dokument ist daher insbesondere für die abhängigen Ansprüche von Interesse.

US 6 196 459 B1 (D8)

In dem Kartenpersonalisierungssystem werden von einem entfernten Personalisierungs-Server 100 die Karten 160 über ihre lokalen Clients 130 personalisiert (siehe Figur 3). Wie in Figur 4 erkennbar, formatiert der Personalisierungsserver 100 die Kommandos für die Karte, welche von dem Client 130 bzw. dessen Schnittstelle zur karte 304 transparent weitergeleitet werden (siehe auch Spalte 5, Zeile 42 - 44 und Spalte 7, Zeile 50 ff). Der Server 100 erhält und verarbeitet anschließend die Kartenantworten. Sowohl für Anspruch 1 als auch für Anspruch 10 stellt das Dokument einen sehr relevanten Stand der Technik dar.

Global Platform – Smart Card Management System (D9)

Diese Systemspezifikation beschreibt Anforderungen an ein Smart Card Management System. Figur 4 zeigt ein System, in welchem ein Remotecomputersystem „Issuer Security Zone" über einen sicheren Kanal „Secure Channel" Daten zur Chipkarte (nicht dargestellt) in dem Client „POS Device" überträgt. Auch hier wird ein Hardware-Sicherheitsmodul HSM verwendet. Insbesondere in den Requirements 6.3.4.1 bis 6.3.4.11 auf Seite 55 und 56 sind einige Aspekte der abhängigen Ansprüche des Streitpatents beschrieben. Zu berücksichtigen ist dabei, dass der Card Manager und die Security Domain Instanzen in der Chipkarte sind (siehe Req. 6.3.4.4 und ggf. ergänzend „Open Platform - Card Specification" Version 2.0.1 vom 7. 04.2000).

Handbuch der Chipkarten (D10)

Dieses Buch ist ein Lehrbuch für den Fachmann auf dem Gebiet der Chipkarten. Es bietet somit einen guten Überblick über das Wissen des Fachmanns. Beispielsweise zeigt es in Bild 12.4 und 12.8 anhand zweier Chipkartensysteme, dass Hardware-Sicherheitsmodule (SAM, PSAM, LSAM, PPSAM) das Mittel der Wahl zur sicheren Schlüsselspeicherung und -verwendung sind.

ETSI TS 101 181 (D11)

Das Dokument D11 ist eine Norm für Mobilfunksysteme und soll zunächst primär aufzeigen, dass auch in einem Mobilfunknetz paket-orientiert (Secure packet structure) Daten transparent von einer entfernten Applikation (bank) zu einem PSD (SIM resident application) übertragen werden. In Abschnitt 8.2 wird explizit die Kodierung der Kartenkommandos als APDU angegeben, die in verpackter Form übermittelt werden.

IV.2 Abhängige Ansprüche

Die Verschlüsselung bzw. entsprechende Entschlüsselung der Daten auf dem Weg zwischen PSD und Remotecomputersystem im Sinne der Merkmale von Anspruch 2 oder 11 ist beispielsweise bekannt aus Dokument D3 oder Dokument D5 (siehe beispielsweise Figur 3 – „verschlüsseln der einzelnen Kommandos"). Gemäß Seite 14 letzter Absatz, Seite 15 vierter Absatz und Anspruch 14 von Dokument D3 erfolgt die

transparente Übertragung zwischen PSD CC und Remotecomputersystem CAS verschlüsselt, die zugehörige Ver- und Entschlüsselung erfolgt also zwangsweise in diesen Einheiten.

Im Sinne von Anspruch 3 beschreibt Dokument D5 in Anspruch 2, dass die Karte als PSD eine eindeutige Kennungsinformationen (Chipkartenidentifikationsdaten) umfasst, aus welcher (mit Hilfe implizit vorhandener Querverweise) das zur Bestimmung der SessionKeys (kryptografische Mittel) zu verwendende Authentisierungsverfahren bestimmt wird.

Die Ansprüche 4 bis 7 betreffen Ausgestaltungen der Initiierung der Kommunikationspipeline. In Dokument D3 erfolgt die Initiierung der Kommunikationspipeline Automatisch nach Verbindung der PSD mit dem Client („Chip kontaktieren" in Figur 2) im Sinne von Anspruch 4, nach einer Anfangsanfrage, die von dem Client erzeugt wurde („Personalisierungsanfrage" in Figur 2) im Sinne von Anspruch 5, und das Einrichten erfolgt im Hintergrund im Sinne von Anspruch 7 (siehe Seite 13 letzter Absatz). In Dokument D8 enthält das Remotecomputersystem 100 Mittel 306 zur Initiierung der Personalisierungsprozesse 308, also auch der Kommunikationspipeline zur Karte 160.

PSD-formatierte Nachrichten werden üblicherweise (auch in Übereinstimmung mit der ISO 7816 für Chipkarten (siehe ggf. Verweis in Dokument D1 auf Seite 13, Zeile 28)) auch als APDU-formatierte Nachrichten bezeichnet (Anspruch 8). Im Bereich von Rechnern ist es üblich, dass Programme über ihre Schnittstelle „API", also auch in diesem Format, Nachrichten austauschen (Anspruch 9).

Die Ansprüche 13 und 14 sind auf die Mittel des Clients und des PSDs respektive gerichtet, die zur Ausführung des Verfahrens gemäß Anspruch 1 nötig sind. Anspruch 15 enthält gegenüber Anspruch 14 zusätzlich nur die für die Schritte von Anspruch 2 nötigen kryptographischen Mittel, deren Existenz in dem PSD zudem zum Prioritätszeitpunkt des Streitpatents für Chipkarten als Selbstverständlichkeit anzusehen ist.

Gemäß Anspruch 12 umfassen die kryptografischen Mittel des Remotecomputersystems ein Hardware Security Module. Die Verwendung von Sicherheitsmodulen ist allgemein üblich, wenn es für die Sicherheit von Daten oder gerade der Schlüssel eines Systems angebracht erscheint. Die Chipkarte selbst ist dabei eine mögliche Form eines Hardware-Sicherheitsmoduls.

Dokument D4 beispielsweise verwendet zu diesem Zweck beispielsweise ein Sicherheitsmodul in dem entfernten Computersystem (siehe „Secure Module" in Figur 6 und „SM 44" in Figur 7).

In Dokument D5 wird der „Schlüssel" als von dem Server-Programm separate Hardwareeinheit dargestellt (siehe Figur 3).

Auch Dokument D7 verwendet ein separates Sicherheitsmodul 3, soweit es angebracht erscheint (siehe Figur 8A).

In Dokument D8 ist es eine „external security source" (siehe Anspruch 6 und Interface 204 in Fig. 2), welche Sicherheitsdienste, wie eine Datenverschlüsselung ermöglichen.

Dokument D9 bezeichnet das Sicherheitsmodul im Remotecomputersystem explizit als HSM (Hardware-Sicherheitsmodul).

Dokument D10 zeigt in Bild 12.4 und 12.8 den Einsatz von Hardware-Sicherheitsmodulen (SAM) an entsprechenden Stellen des jeweiligen Systems.

Zusatzblatt

IX. **Beweismittel**

A. Veröffentlichungen

8 D10: Handbuch der Chipkarten, Rankl/Effing, 3. Auflage 1999, insbesondere S. 622-640

9 D11: ETSI TS 101 181, v 8.3.0 (2000-08), Security Mechanisms for the SIM application toolkit